X.509 Certificate Policy

For The

Health Care PKI

March 6, 2001

Version 0.3.1

Table of Contents

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE

1. INTRODUCTION

This Certificate Policy (CP) defines a "medium level of assurance" for the issuance of digital certificates to be used by agencies in health care applications. The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects the level of trust that the Relying Party can place in a Certificate Authority authorized to operate under this CP.

This CP is modeled after the medium level of assurance expressed in the CP for the Federal Bridge Certification Authority (FBCA) and thus is intended to support interoperability with the FBCA at that level.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

The terms and provisions of this CP shall be interpreted under and governed by applicable Federal law. The United States Government disclaims any liability that may arise from the use of this CP.

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

Certificates issued under this CP contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OID (in this case, the U.S. Government) also publishes the CP, for examination by Relying Parties.

Relationship Between the CP and a Certification Authority CPS

The CP states what assurance can be placed in a certificate issued pursuant to its requirements and expressing its OID. The CPS states how a CA establishes that assurance.

1.2 IDENTIFICATION

There is one level of assurance in this Certificate Policy, defined in subsequent sections. The level has an OID, to be asserted in certificates issued by a Certification Authority (CA) meeting the requirements of this CP. The OID is registered under the id-infosec arc as follows: <NIST to supply>

1.3 COMMUNITY AND APPLICABILITY

This CP applies to certificates issued by agencies for use in the following health care applications: the secure exchange of personally-identifiable healthcare information within agencies (i.e., intraagency), among agencies (interagency), with external business partners (e.g., medical providers filing for Medicare or Medicaid reimbursement) and with private citizens (e.g., a Veteran's or Social Security disability beneficiary's access to medical records in the Agency's possession).

1.3.1 Related Authorities

Agency CAs operating under this CP will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. An agency CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.2 End Entities

1.3.2.1 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates.

1.3.2.2 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.3 Applicability

This CP applies to certificates issued in support of health care applications set forth above.

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

The Federal Public Key Infrastructure Steering Committee is responsible for all aspects of this CP.

1.4.2 Contact person

Questions regarding this CP shall be directed to the Chair of the Federal PKI Steering Committee at fpkisc@gsa.gov.

The FPKI Steering Committee is responsible for determining whether an Agency's CA CPS conforms to this CP and thus may assert the OID set forth above.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

The obligations described below pertain to any agency having responsibility for a CA issuing certificates expressing the OID set forth above.

2.1.1 CA Obligations

Any CA issuing certificates expressing the OID set forth above is responsible for meeting the requirements of this CP.

2.1.2 RA Obligations

An RA who performs registration functions in support of a CA described in 2.1.1 shall also comply with the requirements set forth in this CP.

2.1.3 Subscriber Obligations

Subscribers who receive certificates from CAs described in 2.1.1 shall also comply with the requirements set forth in this CP.

2.1.4 Relying Party Obligations

This CP does not specify what steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own Agency's policies, what steps to take.

2.1.5 Repository Obligations

A CA which issues certificates under this CP may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol,

- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and

- Access control mechanisms when needed to protect repository information as described in later sections.

2.2 LIABILITY

The United States Government disclaims any liability that may arise from use of any certificate issued by Agencies under this CP or its determination to revoke a certificate issued under this CP. In no event will the U.S. Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued under this CP.

2.2.1 Financial Considerations

No Stipulation.

2.2.2 Indemnification by Relying Parties and subscribers

No stipulation.

2.2.3 Fiduciary relationships

No stipulation.

2.2.4 Governing Law

This CP shall be governed by the laws of the United States of America.

2.2.5 Administrative processes

Administrative processes pertaining to this CP shall be determined by the respective agencies.

2.3 INTERPRETATION AND ENFORCEMENT

2.3.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 8.1

2.3.2 Dispute resolution procedures

The FPKI Steering Committee shall resolve any disputes associated with the use of certificates issued under this CP.

2.4 PUBLICATION AND REPOSITORY

2.4.1 Publication of CA Information

The agency responsible for the CA shall publish information concerning that CA necessary to support its use and operation.

2.4.2 Frequency of Publication

Agency certificates are published as specified in this CP. Certificate status information is published as specified in this CP.

2.4.3 Access controls

The Agency CA shall protect any repository information not intended for public dissemination or modification. Public keys and certificate status information in the repository shall be publicly available through the Internet. Access to information in CA repositories shall be determined by the Agency pursuant to its authorizing and controlling statutes.

2.4.4 Repositories

See Section 2.1.5. Compliance Audit

Agency CAs must have a compliance audit mechanism in place to ensure that the requirements of this CP and their CPS are being implemented and enforced.

2.4.5 Frequency of Entity Compliance Audit

The Agency CA and its associated RA(s) shall be subject to a periodic compliance audit which is no less frequent than once per year.

2.4.6 Identity/Qualifications of Compliance Auditor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with applicable requirements.

2.4.7 Compliance Auditor's Relationship to Audited Party

The compliance auditor either shall be a private firm which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to

provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general.

2.4.8 Topics Covered by Compliance Audit

The purpose of a compliance audit shall be to verify that an entity subject to the requirements of this CP is complying with the requirements of this CP.

2.4.9 Actions taken as a result of deficiency

In the event of a material non-conformance with this CP discovered by the Agency, by its compliance auditor, or by some other party, the Agency responsible for the CA issuing certificates under this CP shall immediately notify all parties who may be relying upon the certificates issued by the CA. Procedures for this purpose shall be published by the Agency.

2.4.10 Communication of Result

An Audit Compliance Report, including identification of corrective measures taken or being taken by the Agency, shall be made publicly available, if necessary redacting the information that is inappropriate for public release.

2.5 CONFIDENTIALITY

Information not requiring protection shall be made publicly available. Public access to Agency information shall be determined by the respective Agency.

2.6 INTELLECTUAL PROPERTY RIGHTS

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this CP.

2.7 FEES

The Agency will determine the fees, if any, for Agency CP services.

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of names

The Agency CAs shall generate and sign certificates having an X.500 Distinguished Name (DN); the X.500 DN may also contain domain component elements. Subscribers

shall have a DN assigned through their organizations, in accordance with a naming authority. The X.500 DN shall appear as the subject name; the Alternative Subject Name may also be populated if marked non-critical.

3.1.2 Need for names to be meaningful

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way, preferably that is easily understandable for humans. For people, this will typically include a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

3.1.3 Rules for interpreting various name forms

Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the Agency. The authority responsible for Agency CA name space control shall be identified in the respective CPS.

3.1.4 Uniqueness of names

Name uniqueness across the entire Federal PKI must be enforced. The Agency CA and RA(s) shall enforce name uniqueness within the X.500 name space which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness across the Federal PKI is ensured.

The Agency CAs shall document in its CPS:

- What name forms shall be used, and
- How they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if “Joe Smith” leaves a CA’s community of Subscribers, and a new, different “Joe Smith” enters the community of Subscribers, how will these two people be provided unique names?).

3.1.5 Name claim dispute resolution procedure

The Agency shall resolve any name collisions brought to its attention.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the Agency CA. The Agency CA shall then validate the signature using the party's public key. Other mechanisms that are at least as secure as those cited here may also be employed, as determined by the Agency.

In the case where a key is generated directly on the party's token, or in a key generator that benignly transfers the key to the party's token, then the party is deemed to be in possession of the private key at the time of generation or transfer. If the party is not in possession of the token when the key is generated, then the token shall be delivered to the subject via an accountable method (see Section 6).

When keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The Agency must maintain a record of validation for receipt of the token by the subject. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the Agency CA are the only recipients of this shared secret.

3.1.8 Authentication of organization identity

Requests for Agency CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The Agency RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.1.9 Authentication of Individual Identity

For Subscribers, the Agency CA shall ensure that the applicant's identity information is verified and checked in accordance with this CP and the Agency CA CPS. The Agency CA and/or RA(s) shall ensure that the applicant's identity information and public key are properly bound. Additionally, the Agency CA and/or RA(s) shall record the process that was followed for issuance of each certificate. Process information shall be addressed in the Agency CA CPS. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Subscriber which may be met by establishing how the applicant is known to the verifier as required by this certificate policy;
- A unique identifying number from the ID of the verifier and from the ID of the applicant;

The date and time of the verification.

Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Agency as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement.

Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License).

3.1.10 Authentication of Component Identities

Computing or communications components (routers, firewalls, servers, etc.) may be named as certificate subjects. In such cases, the component must have a human sponsor. The PKI sponsor is responsible for providing the following registration information:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information must be verified. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance).
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements above.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1 Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. Thus, an Agency CA may choose to create a certificate good for one year, renew it twice (each for a one-year period), then re-key at the end of the third year.

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old certificate. For example, an Agency CA may choose to update a certificate of a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent (as set forth above) in order for an updated certificate having the new name to be issued.

Finally, when a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. For self-signed ("root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.1 above.

3.4 REVOCATION REQUEST

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CERTIFICATE

The Agency shall establish and publish procedures for applicants to use in applying for a certificate in its CPS, and shall act upon that application in conformance with the requirements of this CP.

4.1.1 Delivery of public key for certificate issuance

Public keys must be delivered for certificate issuance in a way that binds the applicant's verified identification to the public key. This binding may be accomplished on-line using cryptography. If cryptography is used, it must be at least as strong as that employed in certificate issuance. Additionally, this binding may also be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier or by delivery of a token to a certificate issuer for local key generation at the point of issuance or request. In all cases, the method used for public key delivery shall be set forth in a CPS.

In those cases where public/private key pairs are generated by the Agency CA on behalf of the Subscriber, the Agency CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber. The Agency CA shall also implement procedures to ensure that the token is not activated by an unauthorized entity.

4.2 CERTIFICATE ISSUANCE

Upon receiving a request for a certificate, the Agency CA or RA shall respond in accordance with the requirements set forth in its CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the processes set forth in this CP and the Agency's CPS have been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification.

To the extent practical, certificates once created shall be checked to ensure that all fields and extensions are properly populated. This may be done through software which scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

4.2.1 Delivery of Subscriber's private key to Subscriber

In most cases, a private key will be generated and remain within the cryptographic boundary of the cryptographic module. If the owner of the module generates the key, then there is no need to deliver the private key. If the key is generated elsewhere, then the module must be delivered to the Subscriber. Accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. The Subscriber shall acknowledge receipt of the module. Under no circumstances shall anyone other than the Subscriber have knowledge of or control over private signing keys. Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key. Hardware tokens containing Agency CA private signature keys may be backed-up in accordance with security audit requirements defined below.

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. In these cases:

- An Information Systems Security Officer or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.

- The list of those holding the shared private key must be provided to, and retained by, the applicable CA; and

- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

4.2.2 CA public key delivery and use

The public key of the CA must be available for relying parties to check the signatures on certificates and CRLs issued by the CA. That key will appear in the form of a self-signed root certificate issued by the Agency CA to itself. The Agency CA must ensure that its users receive its self-signed root certificate in a trustworthy fashion. Such a self-signed root certificate is sometimes called a Trusted Certificate. Acceptable methods for Trusted Certificate delivery include but are not limited to:

- The CA loading a Trusted Certificate onto tokens delivered to Relying Parties via secure mechanisms;

- Secure distribution of Trusted Certificates through secure out-of-band mechanisms;

- Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and

- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

4.3 CERTIFICATE ACCEPTANCE

A Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances for revocation of a certificate issued by the Agency CA

A certificate shall be revoked when the binding between the subject and the subject's public key contained within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding include:

- Identifying information in the certificate has become invalid;

- The Subscriber can be shown to have violated, or is suspected of violating, the requirements of this CP;

- The private key has been or is suspected of having been compromised, or has been lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control over the use of the private key.

Additionally, a Subscriber may always request the revocation of his or her certificate directly. Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.4.1.1 Who can request revocation of a certificate issued by an Agency CA

The process for requesting revocation of a Subscriber certificate issued by the Agency CA shall be set forth in the Agency CPS. Revocation normally will proceed once:

- An Agency receives sufficient evidence of compromise or loss of the subscriber's corresponding private key,

- An authenticated request is made to the Agency by the holder of the private key, or

- Someone in his or her supervisory chain, or an officially designated administrative or information security officer, makes an authenticated request for revocation.

4.4.1.2 Procedure for revocation request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

When revocation of a certificate issued by the Agency CA is required, it shall be done within two hours.

4.4.1.3 Revocation of a Certificate Issued by an Agency CA

Revocation shall take effect upon the publication of status information (identifying the reason for the revocation, which may include loss, compromise, or termination of employment) within the time limits as specified in Section 4.4.3 (starting from the time the request is authenticated or sufficient evidence of compromise or loss is received). Information about a revoked certificate shall remain in the status information until the certificate expires and for one additional CRL beyond that point. A certificate may be removed from the second CRL issued after it expires.

4.4.1.4 Revocation Request Grace Period

There is no revocation grace period.

4.4.2 Suspension

Suspension shall not be used by Agency CAs.

4.4.3 Certificate Revocation Lists

All Agency CAs shall issue Certificate Revocation Lists (CRL). To the extent practical, the contents of CRLs shall be checked before issuance to ensure that all information is correct. This may be done using software which scans the CRLs looking for any evidence of an improperly manufactured CRL.

4.4.3.1 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of

certificate status information for off-line or remote (laptop) operation. Agencies shall coordinate with the repositories to which they post certificate status information to reduce latency between creation and availability. Superseded certificate status information shall be removed from the repository system upon posting of the latest certificate status information.

Routine CRLs must be issued at least once each day with additional CRL issuance within 18 hours of notification in the case of lost or compromised private keys.

4.4.3.2 CRL Checking requirements

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.4.4 On-line Revocation / Status checking availability

In addition to CRLs, Agency CAs and Relying Party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

4.4.5 Other forms of revocation advertisements available

No stipulation.

4.4.6 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.7 Special requirements related to key compromise

In the event of an Agency CA private key compromise or loss, the Agency shall immediately notify all parties who may rely upon any certificates issued by that Agency CA.

4.5 SECURITY AUDIT PROCEDURE

Audit log files shall be generated for all events relating to the security of the Agency CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention period for archive,* Section 4.6.2.

4.5.1 Types of Events Recorded

All security auditing capabilities of the Agency CA operating system and PKI CA applications required by this CP shall be enabled. As a result, most of the events identified below shall be automatically recorded. (Note: this list may be replaced in future releases of this CP with a reference to the Certificate Issuing and Management Components Protection Profile being developed by NIST.) At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event.
- The date and time the event occurred.
- A success or failure indicator when executing the Agency CA's signing process.
- A success or failure indicator when executing the Agency CA's signing process.
- A success or failure indicator when performing certificate revocation.
- The identity of the entity and/or operator (of the Agency CA) that caused the event.
- A message from any source requesting an action by the Agency CA is an auditable event. The message must include message date and time, source, destination and contents.

AUDITABLE EVENTS

SECURITY AUDIT

- Any change to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Obtaining a third party time stamp

IDENTIFICATION AND AUTHENTICATION

- Successful and unsuccessful attempts to assume a role
- Change in the value of maximum authentication attempts
- Maximum number of unsuccessful authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from password to biometrics

LOCAL DATA ENTRY

- All security relevant data that is entered in the system

REMOTE DATA ENTRY

- All security relevant messages that are received by the system

DATA EXPORT AND OUTPUT

- All successful and unsuccessful requests for confidential and security relevant information

KEY GENERATION

- Whenever an Agency CA generates a key. (Not mandatory for single session or one time use symmetric keys)

PRIVATE KEY LOAD AND STORAGE

- The loading of Component private keys
- All access to certificate subject private keys retained with the Agency CA for key recovery purposes

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE

- The manual entry of secret keys used for authentication

PRIVATE AND SECRET KEY EXPORT

- The export of private and secret keys (keys used for a single session or message are excluded)

CERTIFICATE REGISTRATION

- All certificate requests

CERTIFICATE REVOCATION

- All revocation requests

CERTIFICATE STATUS CHANGE APPROVAL

- The approval or rejection of a certificate status change request

AGENCY CA CONFIGURATION

- Any security relevant changes to the configuration of the Agency CA

ACCOUNT ADMINISTRATION

- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified

CERTIFICATE PROFILE MANAGEMENT

- All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT

- All changes to the revocation profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile

MISCELLANEOUS

- Installation of the Operating System
- Installation of the Agency CA
- Installing hardware cryptographic modules
- Destruction of cryptographic modules
- System Startup
- Logon Attempts to Agency CA Apps
- Receipt of Hardware/Software
- Attempts to set passwords
- Attempts to modify passwords
- Backing up Agency CA internal database
- Restoring Agency CA internal database
- File manipulation (e.g., creation, renaming, moving)
- Posting of any material to a repository
- Access to Agency CA internal database

- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment of tokens
- Zeroizing tokens
- Rekey of the Agency CA
- Configuration changes to the CA server involving:
    - Hardware
    - Software
    - Operating System
    - Patches
    - Security Profiles

PHYSICAL ACCESS/SITE SECURITY

- Personnel Access to room housing Agency CA
- Access to the Agency CA server
- Known or suspected violations of physical security

ANOMALIES

- Software error conditions
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Electrical power outages
- Uninterruptible Power Supply (UPS) failure

- Obvious and significant network service or access failures
- Violations of Certificate Policy
- Violations of Certificate Practice Statement
- Resetting Operating System clock

4.5.2 Frequency of processing data

Audit logs shall be reviewed at least once every two months. A statistically significant set of security audit data generated by Agency CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

4.5.3 Retention period for security audit data

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the Agency CA system shall be an official different from the individuals who, in combination, command the Agency CA signature key.

4.5.4 Protection of security audit data

The audit process shall not be done by or under the control of the organization responsible for operation of the Agency CA. Agency CA system configuration and procedures must be implemented together to ensure that:

- only authorized people have read access to the logs;
- only authorized people may archive or delete audit logs; and ,
- audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the Agency CA equipment.

4.5.5 Security Audit data backup procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

4.5.6 Security Audit collection system (internal vs. external)

The audit log collection system may or may not be external to the Agency CA system. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Agency shall determine whether to suspend Agency CA operation until the problem is remedied.

4.5.7 Notification to event-causing subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments

No stipulation.

4.6 RECORDS ARCHIVAL

4.6.1 Types of events archived

Agency CA archive records shall be sufficiently detailed to establish the proper operation of the Agency CA, or the validity of any certificate (including those revoked or expired) issued by the Agency CA.

At a minimum, the following data shall be recorded for archive:

- Agency CA accreditation (if applicable)
- Certification Practice Statement
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests

- Subscriber identity Authentication data as per Section 3.1.9
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens
- All certificates issued or published
- Record of Agency CA Re-key
- All CARLs and CRLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

4.6.2 Retention period for archive

The minimum retention period for archive data is 10 years and 6 months. This minimum retention period for these records is intended only to facilitate the operation of the Agency CA.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for a period determined by the Agency.

4.6.3 Protection of archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. The contents of the archive shall not be released except as determined by the Agency or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the Agency CA itself.

4.6.4 Archive backup procedures

No stipulation.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

No stipulation.

4.6.7 Procedures to obtain and verify archive information

Procedures detailing how to create, verify, package, transmit, and store the Agency CA archive information shall be published in the Agency CPS.

4.7 KEY CHANGEOVER

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected.

It is recommended for certificates issued under this CP, the Agency CA signing key have a validity period of three years, and its corresponding certificate have a validity period of six years. An Agency may choose a different signing key validity period but should consider the length of the signing key, how it is protected and controlled, whether their PKI is in a hierarchical or mesh arrangement, and other factors in doing so.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing resources, software, and/or data are corrupted

If the Agency CA equipment is damaged or rendered inoperative, but the Agency CA signature keys are not destroyed, Agency CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

4.8.2 Agency CA signature keys are revoked

If the Agency CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all parties who may be relying upon the certificates shall be notified. The Agency CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in its CPS.

4.8.3 Agency CA signature keys are compromised

If the Agency CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- All Relying Parties and Subscribers shall be immediately and securely notified;

- A new Agency CA key pair shall be generated by the Agency CA in accordance with procedures set forth in the Agency's CPS; and

- New certificates shall be issued to Subscribers in accordance with the Agency CPS.

The Agency CA governing body shall also investigate what caused the compromise or loss, and identify what measures have been taken to preclude recurrence.

4.8.4 Secure Facility impaired after a Natural or Other type of Disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, all Relying Parties and Subscribers shall be immediately and securely notified. The CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing subscriber certificates. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

4.9 CA TERMINATION

In the event that an Agency CA terminates operation, the Agency shall ensure that any certificates issued to that CA have been revoked.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS FOR THE AGENCY CA

CA and RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA and RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the CA and RA equipment environment.

5.1.1 Site location and construction

The location and construction of the facility housing the Agency CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the Agency CA equipment and records.

5.1.2 Physical access

The Agency CA equipment shall always be protected from unauthorized access. The equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

The physical security requirements for the CA are:

- Ensuring no unauthorized access to the hardware is permitted;
- Ensuring all removable media and paper containing sensitive plain-text information is stored in secure containers;
- Being manually or electronically monitored for unauthorized intrusion at all times; and
- Ensuring an access log is maintained and inspected periodically.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and Agency CA equipment shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the Agency CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Electrical Power

The Agency CA shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The Agency CA directories (containing Agency CA issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support a smooth shutdown of the Agency CA operations.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

Agency CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the Agency CA.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

For the Agency CA, full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from the Agency CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational Agency CA.

5.2 PROCEDURAL CONTROLS FOR THE AGENCY CA

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the Agency CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy

and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

Agency CAs may use products from different vendors. Agencies are encouraged to closely examine products before selecting them, and to evaluate those products against the Agency's mission requirements, and then to consider the roles set forth below to ensure that Agency security functions are met. This is particularly important because different commercial products support somewhat different roles and use different mechanisms for registering or enrolling subscribers and issuing certificates. The requirements of this policy are therefore drawn in terms or four, somewhat abstract, roles (Note: the information derives from the Certificate Issuing and Management Components Protection Profile being developed by NIST.):

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. *Officer* – authorized to request or approve certificates or certificate revocations.
3. *Auditor* – authorized to view and maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.

5.2.1.1 Administrator

The administrator role is responsible for:

- installation, configuration, and maintenance of the CA;
- establishing and maintaining CA system accounts;
- configuring certificate profiles or templates and audit parameters, and;
- generating and backing up CA keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Officer

The officer role is responsible for issuing certificates, that is:

- registering new subscribers and requesting the issuance of certificates;
- verifying the identity of subscribers and accuracy of information included in certificates;
- approving and executing the issuance of certificates;
- requesting, approving and executing the revocation of certificates.

5.2.1.3 Auditor

The auditor role is responsible for:

- reviewing, maintaining, and archiving audit logs;
- performing or overseeing internal compliance audits to ensure that the Agency CA is operating in accordance with its CPS.

5.2.1.4 Operator

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.2 Separation of Roles

Role separation may be enforced either by the CA equipment, or procedurally, or by both means.

Role Separation Rules

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, individuals who assume an Officer role may not assume an Administrator or Auditor role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, or an Auditor and an Officer role. No individual shall be assigned more than one identity.

5.2.3 Number of persons required per task

No stipulation.

5.2.4 Identification and authentication for each role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.3 PERSONNEL CONTROLS

5.3.1 Background, qualifications, experience, and security clearance requirements

Each Agency shall identify at least one individual or group responsible and accountable for the operation of each CA in that Agency.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications,

selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the Agency CPS.

Agency CA personnel may hold security clearances if deemed appropriate by their respective Agency.

5.3.2 Background check procedures

Agency background check procedures shall be described in the CPS and shall demonstrate that Agency requirements set forth in Section 5.3.1 are met.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the Agency CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/RA security principles and mechanisms;
- All PKI software versions in use on the CA system;
- All PKI duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

Individuals responsible for PKI roles shall be aware of changes in the Agency CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are Agency CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

The Agency shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the Agency CA or its repository not authorized in this CP or the Agency CPS.

5.3.7 Contracting personnel requirements

Contractor personnel employed to perform functions pertaining to the Agency CA shall meet applicable requirements set forth in the Agency CPS.

5.3.8 Documentation supplied to personnel

The Agency CA shall make available to its CA and RA personnel this CP, relevant parts of the CPS, and any relevant statutes, policies or contracts. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 CA key pair generation

Cryptographic keying material for certificates issued by the Agency CA shall be generated in FIPS 140 Security Level 2 (or higher) validated cryptographic module.

6.1.2 Private Key Delivery to Subscriber

The Agency CA generates its own key pair and therefore does not need private key delivery. Agency CA Subscribers will usually generate their own signature keys and thus will not require delivery; where signature keys are generated by the Agency CA, they will be delivered in accordance with the requirements of this CP and the applicable Agency CP/CPS. For encryption keys, delivery of the private key to the Subscriber (or, if the Subscriber generates the encryption key pair, delivery by the Subscriber to the Agency) shall be in accordance with the requirements of this CP and the applicable Agency CPS.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in an authenticated manner set forth in the CA CPS. This is usually via a certificate electronic request message from an RA, but it may also be done through other secure electronic mechanisms. Further, it may be accomplished via secure non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. If off-line means are used, they shall include identity checking as set forth in this CP and shall also ensure that proof of possession of the corresponding private key is accomplished.

6.1.4 Key sizes

All FIPS-approved signature algorithms shall be considered acceptable.

All certificates issued by Agency CAs shall use at least 1024 bit RSA or DSA, with SHA-1 (or better), in accordance with FIPS 186. Use by the Agency of SSL or another

protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys.

6.1.5 Public key parameters generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

6.1.6 Parameter quality checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186.

6.1.7 Hardware/Software Subscriber key generation

For subscribers, software or hardware shall be used to generate pseudo-random numbers, key pairs and symmetric keys. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.

6.1.8 Key usage purposes (as per X.509 v3 key usage field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalsignature* and *nonrepudiation* bits. Certificates to be used for data encryption shall set the *dataencryption* bit. Agency CA certificates shall set two key usage bits: *cRLSign* and *CertSign*. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management certificates.

Certificates may include a single key for use with encryption and signature in support of legacy Secure Multipurpose Internet Mail Extensions (S/MIME) applications. Such "dual-use" certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such "dual-use" certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. Agencies are encouraged to issue Subscribers two key pairs, one for data encryption and one for digital signature and authentication.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [latest version of FIPS 140 series]. Cryptographic modules shall

be validated to the latest version of the FIPS 140 series level identified in this section. A subscriber's private key may be generated using hardware or software FIPS 140-1 or higher cryptographic module; Agency CA and RA signing keys must be generated using a FIPS 140 level 2 or higher hardware cryptographic module.

6.2.2 CA private key multi-person control

Use of the CA private signing key shall require action by multiple persons as set forth in Section 5.2 of this CP.

6.2.3 Key Escrow of Agency CA private signature key

Under no circumstances shall the Agency CA signature keys used to support non-repudiation services be escrowed by a third party.

6.2.3.1 Escrow of Agency CA encryption keys

No stipulation.

6.2.4 Private Key Backup

6.2.4.1 Backup of Agency CA private signature key

Agency CA private signature keys shall be backed up under the same multi-person control as the original signature key. Such backup shall create only a single copy of the signature key at the CA location; a second copy may be kept at the CA backup location. Procedures to effect this shall be included in the CPS.

6.2.4.2 Backup of subscriber private signature key

Subscriber private signature keys shall not be backed up, escrowed, or copied.

6.2.5 Private Key Archival

Private signature keys shall not be backed up, escrowed, or copied.

6.2.6 Private key entry into cryptographic module

Agency CA private keys shall be generated by and remain in a cryptographic module. The CA private keys may be backed up in accordance with Section 6.2.4.1.

6.2.7 Method of activating private keys

The subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8 Methods of deactivating private keys

If cryptographic modules are used to store subscriber private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.9 Method of destroying subscriber private signature keys

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware should not be required.

6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT

It is technically possible to use the same key-pair for both digital signature and confidentiality. However, this CP discourages that condition, except to support legacy applications as defined in Section 6.1.9. A subscriber's key-pair that is used for digital signatures shall never be escrowed, archived or backed up, because a subscriber can repudiate a transaction if there is a copy of his or her digital signature private key in existence.

For information that is encrypted, the subscriber shall use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the subscriber departs the Agency without relinquishing the private key, or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, an Agency must be able to escrow, backup or archive private keys used for decrypting files and e-mails, while not escrowing, backing up or archiving key-pairs used for authentication. This means that two separate key pairs need to be employed.

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

The CA private signing keys will be used to sign certificates for 3 years.

6.4 ACTIVATION DATA

6.4.1 Activation data generation and installation

The activation data used to unlock Agency CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected. Activation data shall be generated in conformance with FIPS-112. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation data protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account after a predetermined number of failed login attempts as set forth in the CP or CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Agency CA and its ancillary parts shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Require applications to be developed to Trusted Software Development Methodology (TSDM) Level 2
- Restrict access control to CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities

- Prohibit object re-use or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanisms for keys and the CA system
- Enforce domain integrity boundaries for security critical processes

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System development controls

The System Development Controls for the CA are as follows:

- The Agency CA shall use software that has been designed and developed under a development methodology such as MIL-STD-498, the System Security Engineering Capability Maturity Model (SSE CMM), FIPS 140 or the Common Criteria
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase)
- Hardware and software developed for the CA shall be developed in a controlled environment, and the development process shall be defined and documented
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location

- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation

- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security management controls

The configuration of the Agency CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the Agency CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the Agency CA system. The Agency CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Agency CAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the Agency CA.

The Agency CPS shall define the network protocols and mechanisms required for the operation of the Agency CA. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in Section 6.2

7. CERTIFICATE AND CARL/CRL PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version numbers

The Agency CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. Certificate extensions used by the CA shall conform to the Federal certificate profile established by NIST. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. Certificates shall use *Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile* [FPKI-E]. Whenever private extensions are used, they shall be identified in the Agency CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm object identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Certificates containing keys generated for use with DSA or for use with KEA shall be signed with id-dsa-with-sha1. Keys generated for use with RSA shall be signed using sha-1WithRSAEncryption.

7.1.4 Name forms

Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name as specified in [FPKI-E], with the attribute type as further constrained by [RFC2459].

7.1.5 Name constraints

When used, the name constraints extension shall be populated and processed as described in [FPKI-E].

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP will assert the OID associated with this CP (See Section 1.2).

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.2 CRL PROFILE

7.2.1 Version numbers

The Agency CA shall issue X.509 version two (2) CRLs.

7.2.2 CRL entry extensions

Detailed CRL profiles addressing the use of each extension shall conform to [FPKI-E].

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

The Federal PKI Steering Committee (FPKISC) shall review this CP at least once every year. The FPKISC shall maintain and publish a certificate policy plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this CP shall be communicated to every Agency CA subscriber, such communication must include a

description of the change, a change justification, and contact information for the person requesting the change.

All policy changes under consideration by the FPKISC shall be disseminated to interested parties. All interested parties shall provide their comments to the FPKISC in a fashion to be prescribed by the FPKISC.

In evaluating the need for changes to this CP and the object identifiers it contains, FPKISC shall be guided by the language of RFC2527 which states (in section 4.8.1):

It will occasionally be necessary to change certificate policy and certification practice statements. Some of these changes will not materially reduce the assurance that a certificate policy or its implementation provides, and will be judged by the policy administrator as not changing the acceptability of the certificates asserting the policy for the purposes for which they have been used. Such changes to certificate policies and certification practice statements need not require a change in the certificate policy object identifier or the CPS pointer (URL). Other changes to a specification will change the acceptability of certificates for specific purposes, and these changes will require changes to the certificate policy object identifier or CPS pointer (URL).

8.2 PUBLICATION AND NOTIFICATION POLICIES

This CP and any subsequent changes shall be made publicly available within one week of approval.

8.3 CPS APPROVAL PROCEDURES

The term certification practice statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding certificate policy described above.

8.4 WAIVERS

No stipulation.

9. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ABADSG Digital Signature Guidelines, 1996-08-01.

http://www.abanet.org/scitech/ec/isc/dsgfree.html.

FIPS 112 Password Usage, 1985-05-30
http://csrs.nist.gov/fips/

FIPS 140-1 Security Requirements for Cryptographic Modules, 1994-01
http://csrs.nist.gov/fips/fips1401.htm

FIPS 186 Digital Signature Standard, 1994-05-19
http://csrs.nist.gov/fips/fips186.pdf

FOIACT 5 U.S.C. 552, Freedom of Information Act.
Http://www4.law.cornell.edu/uscode/5/552.html

FPKI-E Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997
http://csrs.nist.gov/pki/FPKI7-10.DOC

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996.
Http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990.
Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt
(redacted version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PKCS#12 Personal Information Exchange Syntax Standard, April 1997.
Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.

Federal Bridge Certification Authority Certificate Policy, Dec 2000, Draft

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

Digital Signatures, W. Ford

United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999

10. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile

FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology

UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

11. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an "applicant" after applying

	to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity recognized by the Federal PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.

Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting,

	compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an

	object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields;

	"date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Agency as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Agency Principal Certification Authorities.
Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the

	FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in

	the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO

	registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. Each Agency shall be responsible for identifying an internal component charged with these responsibilities
Principal CA	The Principal CA is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA, one of which may be a healthcare CA issuing certificates under this CP.

Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known

	as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

12. ACKNOWLEDGEMENTS

While a large number of people identified below participated in the review and development of this Certificate Policy, we would like to specially thank Ms. Rebecca Kahn, of the Federal Public Key Infrastructure Steering Committee.

Judith Spencer GSA judith.spencer@gsa.gov

Daniel Chenok	OMB	Daniel J. Chenok @omb.eop.gov
Brian Burns	HHS	Bburns@os.dhhs.gov
Brian Kelly	OSD	Brian.kelly@tma.osd.mil
Emma Clark	OSD	Emma.clark@tma.osd.mil
David Temoshok	GSA	David.temoshok@gsa.gov
Don Bartley	HCFA	Dbartley@hcfa.gov
Donna Dodson	SSA	Ddodson@ssa.gov
Eleanor Bell	OSD	Eleanor.bell@tma.osd.mil
Jonathan Womer	OMB	Jonathan_p._womer@omb.eop.gov
Richard Church	HHS	Richard.church@mail.his.gov
Richard Kellet	GSA	Richard.kellett@gsa.gov
Robert Kolodner	VA	Robkolodner@hq.med.va.gov
Ruth Anderson	VA	Ruth.anderson@mail.va.gov
Victoria Quigley	HCFA	Vquigley@hcfa.gov
Daniel Maloney	VA	Daniel.maloney@med.va.gov